## REMARKS

Claims 17-21, 26-27, and 33-40 were pending in this application prior to the final Office Action. By this amendment, claims 17-21 and 26-27 are canceled, claims 33, 36, and 39 are amended, and new claims 41-46 are added. No new matter has been added. Thus, claims 33-46 are now pending. In view of the following remarks, reconsideration and allowance of the application is respectfully requested.

Claim 39 stands objected to because the Examiner asserts that the term "analyses" should be replaced with term "analyzed". Claim 39 is amended herein according to the Examiner's recommendation. Thus, this objection is believed to be overcome.

In addition, claims 36 is amended to correct a typographical error. Specifically, "located mobile devices or resources" should be "detected mobile devices or resources." No new matter has been added.

Claims 17-21 and 26-27 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Albert et al (2003/0177389). However, in view of the cancellation of claims 17-21 and 26-27 herein, Applicants believe this rejection is now moot, and should be withdrawn.

Claims 33-40 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Albert in view of Sharma et al (2002/0068559). In particular, the Examiner asserts that Albert discloses using the determined mobile device information for managing security of the computer system (see, for example, [00011]; [00014]; [0024]), and that Sharma discloses a method for managing a computer system including a computing node and one or more mobile devices (see, for example, abstract; [0010]-[0012]), comprising running a discovery program to detect one or more mobile devices or resources (see, for example, [0061]-[0062]; [0066]-[0067]), and determining information regarding one or more mobile devices or resources based on at least one of a registry resource, a file resource, a process resource, a network management parameter, a data format, a packet format, a synchronization log entry, a directory structure, a database entry, the presence of an executable program and attributes associated with a mobile device or resource (see, for example, [0020]; [0039]; [0047]; [0064]). Thus, the Examiner asserts that it would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement in the system of Albert, a

computer system management program for the discovery and detection of mobile devices in the system as taught in Sharma, because it would provide a mechanism to manage network assets via a secure communication path (Sharma, [0010]).

In addition, the Examiner asserts that Sharma discloses a server capable of finding the location of a particular asset (corresponding to the recited mobile device or resource) (e.g. [0008]), and that Sharma further discloses a network management server that includes a module called network discovery process (e.g. Fig. 4, block 426) that is capable of discovering the network physical assets and links (corresponding to the recited detect one or more mobile devices or resources) (e.g. [0071]).

However, Applicants respectfully submit that neither Albert nor Sharma, alone or in combination, disclose, suggest, or render obvious the invention recited in claims 33-46, as presented herein.

In particular, as stated by the Examiner, Albert fails to disclose or suggest any sort of discovery program, which is recited in the claims. Instead, Albert merely relates to a series of methods that allow a mobile device to apply a security policy required for connection to a particular network (i.e. an end-point security system that formalizes the interaction from a user client-side device of policies required by the user for his device). More specifically, Albert relates to network security problems regarding connecting PCs, Laptops, and Mobile Devices to various networks that have different security requirements. (See paragraph [0009]).

Sharma discloses, for example, in paragraph [0066], the use of a "network discovery function" which browses the network to discover the existing network topology. The network topology serves as a schematic or blueprint of the assets present on the network. Thus, the discovery function of Sharma browses the network and discovers assets that *exist* or are *present* on the network. There is no suggestion whatsoever in Sharma that the network discovery function is capable of detecting "one or more mobile devices or resources connected to the network connection" and "one or more mobile devices or resources previously, but not currently, connected to the network connection" as is recited in claim 33. Specifically, Sharma fails to disclose or suggest at least that mobile devices or resources that were previously connected to the network, but are not currently connected to the network, can

be detected.

In contrast, the present invention relates to a method for managing a computer system including, in relevant part, running a discovery program to detect one or more mobile devices or resources connected to the network connection and one or more mobile devices or resources previously, but not currently, connected to the network connection.

As is stated in the Specification, starting on line 28, on page 17, a *discovery process is used to discover, detect, or locate mobile devices 104*, resources based on specified discovery rules. Various methods can be used to detect and discover the mobile devices 104 or resource devices 124. In addition, the discovery program *discovers, detects, or locates one or more mobile devices or other resources that at one time or another have attached to the system*, such as a USB flash, memory or SD card storage media (or any other resource) that can attached to the computing node 102 or the mobile devices 104 using well known protocols. Furthermore, information regarding discovered, detected, or located mobile device or resources is determined based on any one of a registry resource, a file resource, a process resource, a network management parameter, a communication protocol parameter, a data format, a packet format, a synchronization log entry, a directory structure or a database entry. The mobile devices or external resources can leave an imprint in the registry structure any time they attach to a computing node. The imprint is not erased when a device disconnects. Thus, *any device that has attached to the computing node at any time in the past can be detected and identified.*

Thus, for at least the above reasons, neither Albert nor Sharma, alone or in combination, disclose, suggest, or render obvious the invention recited in pending claims 33-46. Therefore, Applicants respectfully request that the rejection of claims 33-46 under 35 U.S.C. § 103(a) as being unpatentable in view of Albert and Sharma be reconsidered and withdrawn.

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. If, however, the Examiner deems that any issue remains after considering this response, the Examiner is invited to contact the undersigned attorney to expedite the prosecution and engage in a joint effort to work out a mutually satisfactory solution.

Except for issue fees payable under 37 C.F.R. § 1.18, the Commissioner is hereby authorized by this paper to charge any additional fees during the entire pendency of this application including fees due under 37 C.F.R. §§ 1.16 and 1.17 which may be required, including any required extension of time fees, or credit any overpayment to Deposit Account No. 19-2380. This paragraph is intended to be a CONSTRUCTIVE PETITION FOR EXTENSION OF TIME in accordance with 37 C.F.R. § 1.136(a)(3).

Respectfully submitted,

NIXON PEABODY, LLP

Date: June 12, 2007

/Stephen M. Hertzler, Reg. No. 58,247/
Stephen M. Hertzler

**NIXON PEABODY LLP**
Customer No. 22204
401 9th Street, N.W., Suite 900
Washington, D.C. 20004
(202) 585-8000